VERFASSUNGSGERICHTSHOF
B 1031/11-20
29. Juni 2012

IM NAMEN DER REPUBLIK!

Der Verfassungsgerichtshof hat unter dem Vorsitz des Präsidenten
Dr. Gerhart HOLZINGER,

in Anwesenheit der Vizepräsidentin
Dr. Brigitte BIERLEIN

und der Mitglieder
Mag. Dr. Eleonore BERCHTOLD-OSTERMANN,
Dr. Sieglinde GAHLEITNER,
DDr. Christoph GRABENWARTER,
Dr. Christoph HERBST,
Dr. Michael HOLOUBEK,
Dr. Helmut HÖRTENHUBER,
Dr. Claudia KAHR,
Dr. Georg LIENBACHER,
Dr. Rudolf MÜLLER,
DDr. Hans Georg RUPPE,
Dr. Johannes SCHNIZER

sowie des Ersatzmitgliedes
Dr. Nikolaus BACHLER

als Stimmführer, im Beisein der Schriftführerin
Dr. Martina WEINHANDL,

in der Beschwerdesache des Johannes Albrecht G., (...), Wien, vertreten durch Rechtsanwalt Dr. Helmut Graupner, Maxing-straße 22-24/4/9, 1130 Wien, gegen den Bescheid der Datenschutzkommission vom 20. Juli 2011, Z DSK-K121.697/0008-DSK/2011, in seiner heutigen nichtöf-fentlichen Sitzung gemäß Art. 144 B-VG zu Recht erkannt:

I. Der Beschwerdeführer ist durch den angefochtenen Bescheid weder in einem verfassungsgesetzlich gewährleisteten Recht noch wegen Anwendung einer rechtswidrigen generellen Norm in seinen Rechten verletzt worden.

II. Die Beschwerde wird abgewiesen.

Entscheidungsgründe

I. Sachverhalt, Beschwerdevorbringen, Vorverfahren

1. Der Beschwerdeführer kommunizierte am 11. November 2009 im Internet von seinem PC aus unter einem Benutzernamen ("Nickname") in einem auf sexuelle Kontakte spezialisierten Chatroom mit der ihm zugeteilten Internetprotokolladresse (IP-Adresse). Hiebei erweckte er bei einem Chatpartner den Eindruck, unmündige Personen, nämlich "7-11jährige, oder wenn gewünscht auch jünger", zu sexuellen Handlungen anzubieten. Von diesem Sachverhalt wurde das Landeskriminalamt Wien unter Bekanntgabe der Internetseite (domain) und des vom Beschwerdeführer verwendeten "Nickname" informiert. Die befassten Beamten der Bundespolizeidirektion Wien (BPD Wien) gingen von einer konkret und unmittelbar drohenden Gefahr für die Sicherheit Unmündiger aus und ermittelten zunächst auf Grundlage des § 53 Abs. 3a Z 2 des Bundesgesetzes über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), BGBl. 566/1991 idF BGBl. I 114/2007, im Wege einer sogenannten Whois-Abfrage beim Domaininhaber die Website, sodann anhand dieser und des "Nickname" über den technischen Betreiber des Chatservers die konkrete IP-Adresse des Endgerätes, von dem aus die Nachricht versendet wurde, samt Login-Zeitpunkt. Auf Grund dieser Daten konnte gemäß § 53 Abs. 3a Z 3 SPG im Wege einer weiteren Whois-Abfrage der Provider, dem die IP-Adresse (innerhalb eines Adressenblocks) zugeordnet war 1

(UPC Austria GmbH), und über diesen schließlich Namen und Adresse des Beschwerdeführers (als Anschlussinhaber und Benutzer) ausgeforscht werden. Er und eine Reihe weiterer Personen wurden wegen des Verdachts der versuchten Bestimmung zum schweren sexuellen Missbrauch von Unmündigen sowie zur entgeltlichen Förderung fremder Unzucht (§§ 15, 12 iVm § 206 und § 214 StGB) bei der Staatsanwaltschaft Wien zur Anzeige gebracht.

2. Insbesondere iZm der Ermittlung der IP-Adresse brachte der Beschwerdeführer gegen die BPD Wien und gegen das Landespolizeikommando Wien (LPK Wien) bei der Datenschutzkommission (DSK) Beschwerde u.a. wegen Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten ein, in der vor allem mit der Behauptung eines Eingriffs in das gemäß Art. 10a StGG verfassungsgesetzlich geschützte Fernmeldegeheimnis das Fehlen einer bei verfassungskonformem Verständnis des § 53 Abs. 3a Z 2 SPG (bzw. mit Blick auf § 18 Abs. 2 E-Commerce-Gesetz – ECG) erachteten gerichtlichen Bewilligung gerügt wird. 2

3. Die DSK wies die Beschwerde mit Bescheid vom 20. Juli 2011 teils (in Bezug auf die BPD Wien) ab (Spruchpunkt 1.), teils (hinsichtlich des LPK Wien, Landeskriminalamt mangels Auftraggebereigenschaft) zurück (Spruchpunkt 2.). Begründend wird (mit Bezugnahme auf die Rechtsprechung des Obersten Gerichtshofes) ausgeführt, dass sämtliche Voraussetzungen zur Ausforschung der Daten iSd (nicht unter Richtervorbehalt stehenden) § 53 Abs. 3a Z 2 und 3 SPG vorgelegen seien: Das Verhalten des Beschwerdeführers habe eine Gefahrenlage iSd § 21 Abs. 2 SPG befürchten lassen, bei den Auskunft erteilenden Unternehmen handle es sich um Diensteanbieter iSd § 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 (TKG 2003) bzw. § 3 Abs. 2 ECG; der Eingriff sei auch verhältnismäßig gewesen. § 53 Abs. 3a SPG gehe dem (unter Richtervorbehalt stehenden) § 18 Abs. 2 ECG zufolge § 18 Abs. 5 ECG vor. Die Prüfung der angewendeten Vorschriften auf ihre Verfassungskonformität liege außerhalb der Befugnisse der DSK. 3

4. (Nur) gegen Spruchpunkt 1. dieses Bescheides richtet sich die gemäß Art. 144 B-VG erhobene Beschwerde, in der die Verletzung verfassungsgesetzlich gewährleisteter Rechte, primär des Fernmeldegeheimnisses (Art. 10a StGG), ferner des Rechts auf Geheimhaltung personenbezogener Daten (§ 1 Abs. 1 DSG 2000), auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) und auf Gleichheit aller Staatsbürger vor dem Gesetz (Art. 2 StGG, Art. 7 B-VG, Art. 14 EMRK), allenfalls 4

auch in Rechten wegen Anwendung eines verfassungswidrigen Gesetzes, geltend gemacht wird:

Bei IP-Adresse und Benutzernamen handle es sich um Verkehrsdaten iSd § 92 Abs. 3 Z 4 TKG 2003. Da der Betreiber des Chatroom für die Ermittlung dieser Daten seine "Logfiles" (Protokoll-Dateien bzw. Authentifizierungsdaten) durchsuchen müsse, würden die verlangten Auskünfte dem Richtervorbehalt des Art. 10a StGG unterliegen; diese Verfassungsbestimmung gelte auch für Stammdaten. § 53 Abs. 3a Z 2 SPG sei verfassungskonform dahin zu verstehen, dass zumindest die Ermittlung von IP-Adressen einer gerichtlichen Bewilligung bedürfe. Andernfalls wären die angewendeten Rechtsvorschriften verfassungswidrig. 5

5. Die belangte Behörde legte die Verwaltungsakten vor und erstattete eine Gegenschrift, in der sie die Abweisung der Beschwerde beantragt. Der DSK komme keine Entscheidungsbefugnis in Bezug auf allfällige Eingriffe in das Fernmeldegeheimnis zu. Die Frage, ob die ermittelten Daten zum Kern des Fernmeldegeheimnisses (Inhaltsdaten einer über öffentliche Netze laufende Kommunikation) oder zum (unterschiedlich weit verstandenen) sonstigen Schutzbereich (Stamm-, Verkehrs- bzw. Verbindungsdaten) zählen, sei nicht relevant, da das DSG 2000 keine Unterscheidung hinsichtlich dieser Datengruppen treffe und die bekämpfte Ermittlung jedenfalls von der Ermächtigung des § 53 Abs. 3a SPG gedeckt gewesen sei. Das Gesetz erlaube Sicherheitsbehörden, in Konstellationen wie der vorliegenden anhand einer bestimmten Nachricht sowohl die IP-Adresse (beim Betreiber des Chatservers als "sonstigen Diensteanbieter" – § 3 Z 2 ECG) als auch Namen und Anschrift des Benutzers (beim ISP/Access-Provider als "Betreiber eines öffentlichen Telekommunikationsdienstes" – § 92 Abs. 1 Z 1 TKG 2003) ohne Gerichtsbeschluss zu ermitteln. Der angestrebten, auf das Erfordernis der Einholung einer gerichtlichen Bewilligung abzielenden Deutung stehe der klare Wortlaut des § 53 Abs. 3a SPG entgegen. § 18 Abs. 2 ECG habe einen anderen Regelungsgegenstand, sei lex posterior und lasse Auskunftspflichten gegenüber Sicherheitsbehörden ausdrücklich unberührt. 6

6. Der Verfassungsgerichtshof richtete an die Bundesministerin für Inneres einzelne (nachstehend wiedergegebene) Fragen, zu denen folgende Stellungnahme erging: 7

"Einleitend ist festzuhalten, dass das Fernmeldegeheimnis nach Art 10a StGG die Vertraulichkeit der auf einem bestimmten Kommunikationsweg übermittelten Information schützt. Der verfassungsrechtliche Schutz beschränkt sich demnach auf die Inhalte der Kommunikation, genauer gesagt, auf alle nicht für die Öffentlichkeit bestimmten Informationen, die im Wege des Fernmeldeverkehrs übermittelt werden. Nicht davon umfasst sind nach herrschender Meinung (vgl Wiederin in Korinek/Holoubek [Hrsg], Österreichisches Bundesverfassungsrecht, Art 10a StGG Rz 12) und strafgerichtlicher Rechtsprechung (OGH 13.4.2011, 15 Os 172/10y, 15 Os 173/10w; JBI 2011, 726) äußere Aspekte der Kommunikation, wie etwa die mit einer Kommunikation anfallenden Verbindungsdaten. Diese Ansicht kommt auch im Beschluss des VfGH vom 1. Juli 2009 zum Ausdruck, indem festgehalten wird, dass die Bestimmungen des § 53 Abs 3a und 3b SPG nicht die 'geheime Überwachung des Fernmeldeverkehrs' gestatten und keine Grundlage für die Ermittlungen von Inhaltsdaten bieten (VfGH 1.7.2009, G 147, 148/08-14, Seite 34).
Eine Verletzung des Fernmeldegeheimnisses durch die Bestimmungen des § 53 Abs 3a SPG läge nur dann vor, wenn der Staat in die Vertraulichkeit der übermittelten Information durch das Einholen der Auskunft eingreifen würde. Dabei kommt zunächst einmal der Tatsache wesentliche Bedeutung zu, dass nur jene nicht für die Öffentlichkeit bestimmten Informationen dem Grundrechtsschutz unterliegen. Für den hier in Rede stehenden Bereich der Internetkommunikation bedeutet dies, dass jedenfalls der E-Mail Verkehr und die Internet-Telefonie vom Schutzbereich des Fernmeldegeheimnisses erfasst sind, nicht aber jene Informationen, die auf einer öffentlich zugänglichen Homepage, in offenen Foren oder Newsgroups, Blogs etc preisgegeben werden, weil diese für die Öffentlichkeit bestimmt sind. Demgegenüber ist bei Chat-Foren nach Wiederin zu differenzieren, ob es sich um offene oder geschlossene Foren (Privat-Chat) handelt (Wiederin in Korinek/Holoubek [Hrsg], Österreichisches Bundesverfassungsrecht, Art 10a StGG Rz 7). Kennzeichnend für geschlossene Foren ist, dass diese nur einem beschränkten Teilnehmerkreis offen stehen und die Teilnahme an der Kommunikation in der Regel an die Erteilung einer gesonderten Berechtigung (eventuell unter Verwendung einer Verschlüsselung) geknüpft ist.
Das entscheidende Gewicht bei der Interpretation des Befugnisumfangs kommt aber dem Wortlaut des § 53 Abs 3a Z 2 SPG idF BGBl I 114/2007 zu (vgl die ausdrückliche Aufzählung der sicherheitspolizeilichen Aufgaben in den lit a bis c der Z 2 und 3 des § 53 Abs 3a SPG idF BGBl I 33/2011 und den Bericht des Justizausschusses, 1124 BlgNR 24. GP). Dieser ermächtigt die Sicherheitsbehörden über die IP-Adresse zu einer bestimmten Nachricht (und den Zeitpunkt ihrer Übermittlung) Auskunft zu verlangen. Anknüpfungs- und Ausgangspunkt in allen Fällen des § 53 Abs 3a SPG ist, dass der Inhalt der Kommunikation (Tatsachen, die die Annahme einer konkreten Gefahrensituation rechtfertigen, etwa angekündigter Selbstmord oder Verdacht eines gefährlichen Angriffs) der Sicherheitsbehörde im Zeitpunkt der Anfrage bereits bekannt ist (siehe dazu die Stellungnahme der Bundesregierung an den VfGH, GZ BKA-604.310/0009-V/5/2008). Das bedeutet, dass durch die Beauskunftung nach § 53 Abs 3a SPG nicht – anders als bei einer Überwachungsmaßnahme gemäß § 134 Z 3 StPO – die Kommunikation als solche erst bekannt wird, sondern es durch die Beauskunftung lediglich zur Zuordnung einer Kommunikation bekannten Inhalts zum Absender kommt.

Der Begriff 'bestimmte Nachricht' ist im Sinne einer verfassungskonformen Interpretation eng auszulegen. In Anlehnung an den Wortlaut des § 119 StGB bedeutet das Abstellen auf eine 'bestimmte Nachricht' in § 53 Abs 3a Z 2 SPG, dass es sich zum einen um die Mitteilung einer Gedankenerklärung (Lewisch in WK^2 § 119 Rz 9a) von einem Menschen an (einen) andere(n) Menschen unter Verwendung des Internet Protokolls handeln muss und zum anderen, dass eine Nachricht nur dann bestimmt ist, wenn sie der Sicherheitsbehörde tatsächlich bereits vorliegt (Feiler, in Zankl [Hrsg], Auf den Weg zum Überwachungsstaat?, Die Befugnisse des § 53 Abs 3a SPG, 73). Kenntnis vom Inhalt der Nachricht erhält die Sicherheitsbehörde entweder über Aufforderung eines Dritten (dabei handelt es sich in der Regel um den Empfänger der Nachricht) oder durch eigene Wahrnehmung in der virtuellen Öffentlichkeit, wodurch der Inhalt der Nachricht als nicht mehr geheim im Sinne des Art 10a StGG zu beurteilen ist. Aufgrund der strikten Bindung der Ermächtigungen des SPG an das Vorliegen einer Aufgabe kommt ein Einschreiten ohne Vorliegen einer bestimmten Nachricht iS eines SPG-relevanten Sachverhalts, aus dem sich eine sicherheitspolizeiliche Aufgabe ergibt, nicht in Betracht.

<u>Zu den einzelnen Fragen:</u>

1) Wie stellt sich der konkrete Ablauf der Ermittlungen einer dynamischen IP-Adresse sowie der Ausforschung von Namen und Adresse des Inhabers des Endgeräts, dem eine bestimmte IP-Adresse zugeordnet ist, dar?
Wie einleitend erwähnt, ist Anknüpfungs- und Ausgangspunkt in allen Fällen des § 53 Abs 3a SPG, dass der Inhalt einer Kommunikation (etwa angekündigter Selbstmord oder Verdacht von Kindesmissbrauch) der Sicherheitsbehörde zur Kenntnis gelangt ist. Um die sicherheitspolizeilichen Aufgaben (Gefahrenabwehr, EAH) erfüllen zu können, ist es notwendig, den Absender der Nachricht zu ermitteln.
Zu diesem Zweck wird der Diensteanbieter (§ 3 Z 2 E-Commerce-Gesetz) der betroffenen Internet-Domain (Chatroom-, Blog-, Homepage-Betreiber), der durch eine WHOIS-Anfrage (Whois [englisch who is 'wer ist'] ist ein Protokoll, mit dem von einem verteilten, öffentlich zugänglichen, Datenbanksystem Informationen zu Internet-Domains und IP-Adressen und deren Eigentümern abgefragt werden können.) herauszufinden ist, gem § 53 Abs 3a Z 2 SPG aufgefordert, die IP-Adresse und den genauen Zeitpunkt der Übermittlung bekannt zu geben. Im Durchführungserlass GZ 94.762/101-GD/08 (Beilage 1), seit 1.4.2012 ersetzt durch den Erlass GZ BMI-KP1000/0233-II/8/2012 (Beilage 2), sind die Anfragekriterien von Seiten der Sicherheitsbehörde (Nickname und der Zeitraum der Übermittlung, bei Einträgen in Chats oder Foren auch der Name des 'Raumes') erläutert und die Anfrage selbst ist ausschließlich mittels Formular (Anlage 1 der Erlässe) zu stellen. Als Antwort erhält die Sicherheitsbehörde im Wege des ausgefüllten Formulars die angefragte IP-Adresse zur vorliegenden Nachricht und den Zeitpunkt der Übermittlung.
Anhand dieser Kriterien wird durch eine neuerliche WHOIS-Anfrage der Betreiber eines öffentlichen Kommunikationsdienstes (idR ein Internet-Zugangsdienst iSd § 92 Abs 3 Z 14 TKG 2003) dieser IP-Adresse ermittelt. Anschließend wird dieser gem § 53 Abs 3a Z 3 mittels in Beilage 1 übermittelten Formulars aufgefordert,

Name und Anschrift des Benutzers mitzuteilen, dem diese IP-Adresse zum Zeitpunkt der Nachrichtenübermittlung zugewiesen war.
Das SPG unterscheidet bei der Beauskunftung von IP-Adressen nicht, ob diese statisch oder dynamisch (Stamm- oder Zugangsdatum) vergeben wurden, da der Betreiber mittels beiliegenden Formulars immer nur Name und Anschrift beauskunftet.

2) Ist eine gemäß § 53 Abs 3a Z 2 SPG gesuchte IP-Adresse von anderen Inhalten (als der schon bekannten Nachricht) technisch trennbar bzw ist gewährleistet, dass der Sicherheitsbehörde vom Betreiber oder sonstigen Diensteanbieter ausschließlich die IP-Adresse (ohne Inhalte) übermittelt wird?
Das in der Beilage 1 übermittelte Formular für die Anfrage an Betreiber/Diensteanbieter ist hinsichtlich der Fragestellung durch die Sicherheitsbehörde und Antwortmöglichkeit der Anbieter ausdrücklich auf die im § 53 Abs 3a SPG normierten Datenarten beschränkt (Name, Anschrift, Teilnehmernummer, IP-Adresse und Zeitpunkt der Übermittlung der vorliegenden Nachricht). Für die Erlangung anderer Datenarten, insbesondere Kommunikationsinhalte, als der schon bekannten Nachricht enthält § 53 Abs 3a SPG keine Ermächtigung.
Die technische Trennbarkeit der IP-Adresse von anderen Inhalten beim Betreiber bzw Diensteanbieter (interne Abfragekriterien, Logvorgänge, Protokollierung etc) kann von Seiten des BMI nicht beantwortet werden, da die technischen Spezifikationen im Rahmen der Vorgaben des TKG 2003 (siehe Beantwortung zur Frage 3) in der Ingerenz der Betreiber bzw Diensteanbieter liegen.

3) Ist gewährleistet, dass der Sicherheitsbehörde gem § 53 Abs 3a Z 3 SPG vom Betreiber oder sonstigen Diensteanbieter ausschließlich Name und Anschrift des Inhabers des Endgeräts, dem eine bestimmte IP-Adresse zugeordnet ist, ohne Inhaltsdaten bekannt gegeben werden?
Siehe die Beantwortung zu Frage 2 über die Verwendung eines Formulars, aus dem sich Anfragekriterien und die zu beauskunftenden Datenarten ergeben. Darüber hinaus wird auf die restriktiven Regelungen der §§ 99 ff TKG 2003 über die Zulässigkeit der Speicherung von Daten (Verkehrs- Standort bzw. Inhaltsdaten) - abhängig von der Erbringung des jeweiligen Dienstes - verwiesen. Gemäß § 101 TKG 2003 dürfen reine Zugangsprovider (siehe zur Definition des Internet-Zugangsdienstes § 92 Abs 3 Z 14 TKG 2003) keine Inhaltsdaten speichern.

4) In welchen Fällen sind der Sicherheitsbehörde außer der IP-Adresse auch der Inhalt oder Teile des Inhalts der mit einer IP-Adresse verbundenen Nachricht bekannt bzw sind IP-Adressen und die dazugehörigen Nachrichten soweit trennbar, dass der Sicherheitsbehörde ausschließlich die IP-Adresse bekannt wird?
Wie eingangs bereits ausgeführt, liegt jeder Beauskunftung zu einer IP-Adresse eine bestimmte Nachricht zugrunde, von der die Sicherheitsbehörde entweder durch eigene Wahrnehmung in der virtuellen Öffentlichkeit oder durch einen Hinweisgeber (Chatpartner, Empfänger der Email) Kenntnis erlangt hat und durch die sich eine sicherheitspolizeiliche Aufgabenstellung ergibt.
Denkbar ist, dass der Sicherheitsbehörde zugleich mit dem Inhalt der Nachricht auch die IP-Adresse des Betroffenen bekannt gegeben wird, etwa bei Vorlage eines Emails mit dem gesamten 'Header', in dem die IP-Adresse ersichtlich ist.

Technisch möglich ist es auch für einen Chatteilnehmer, die IP-Adresse eines Kommunikationspartners herauszufinden.
Aus einer bekannt gegebenen IP-Adresse ohne dazugehörige Nachricht lässt sich eine sicherheitspolizeiliche Aufgabenstellung nicht ableiten.

5) Welche Kategorien offener oder geschlossener Kommunikation im Internet lassen sich unter den hier zu beurteilenden rechtlichen Gesichtspunkten bilden?
Grundsätzlich sind alle Foren und Chats (auch Blogs, soziale Netzwerke wie Facebook, Google+, Twitter etc.) öffentlich zugänglich. Bei diesen Diensten handelt es sich somit grundsätzlich um eine offene, für alle Teilnehmer zugängliche und damit 'sichtbare' Kommunikation. Bei den meisten dieser Dienste muss man sich zunächst nur anhand einer Email-Adresse (kann auch eine Fantasieadresse sein) registrieren. Im Zuge dieser Registrierung wird zusätzlich ein Nickname (=Spitznamen, z.B. 'mausi1') gewählt, der die Kommunikationsteilnehmer unterscheidbar macht. Diese Art der Kommunikation ist als offen zu werten, sodass ein Eingriff ins Fernmeldegeheimnis ausgeschlossen ist.
Steht ein gesondert zur Verfügung gestellter (Kommunikations-)Bereich nur besonders Berechtigten (etwa durch eigene Passwörter geschützt) zur Verfügung, oder bietet der Chatbetreiber einen geschlossenen Kommunikationsbereich (sog. Privat-Chat) an, der auch zusätzlich verschlüsselt sein kann und welcher dann nur einem eingeschränkten Personenkreis zugänglich ist (im Extremfall gibt es nur zwei Kommunikationspartner), so spricht man von geschlossener Kommunikation. Wenn ein solcher Kommunikationsinhalt, aus der sich eine sicherheitspolizeiliche Aufgabe ergibt, der Sicherheitsbehörde durch einen der Teilnehmer bekannt gegeben wird, ist auch in diesem Fall kein Eingriff ins Fernmeldegeheimnis durch die Sicherheitsbehörde erfolgt.

6) Ermächtigt § 53 Abs 3a SPG zur Ermittlung von IP-Adressen ohne Differenzierung danach, ob die Übermittlung der Mitteilung von E-Mails, der IP-Telefonie, der Teilnahme an einem offenen oder geschlossenen Internetforum oder der bloßen Abfrage von öffentlichen Webseiten uä dient?
Es wird auf die einleitenden Ausführungen zur Notwendigkeit des Vorliegens einer bestimmten Nachricht verwiesen; aus welchem Kommunikationsvorgang (E-Mail oder Forum) die Nachricht stammt, ist irrelevant, da der Inhalt der 'bestimmten Nachricht' nicht unter Durchbrechung des Fernmeldegeheimnisses auf Grundlage des SPG durch die Sicherheitsbehörde ermittelt wurde. Die Abfrage von öffentlichen Webseiten kann jedenfalls nicht auf § 53 Abs 3a SPG gestützt werden."

7. Der Beschwerdeführer erstattete dazu eine Stellungnahme, in der er im Wesentlichen sein bisheriges Vorbringen wiederholt. 8

II. Rechtslage

1. Art. 10a StGG idF BGBl. 8/1974 lautet: 9

"Das Fernmeldegeheimnis darf nicht verletzt werden.
Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig."

2. Hier wesentliche Bestimmungen des Sicherheitspolizeigesetzes, BGBl. 566/1991 idF BGBl. I 131/2009, lauten: 10

"1. TEIL

[...]

3. Hauptstück
Begriffsbestimmungen

Allgemeine Gefahr; gefährlicher Angriff; Gefahrenerforschung

§ 16. (1) Eine allgemeine Gefahr besteht
1. bei einem gefährlichen Angriff (Abs. 2 und 3)
oder
2. sobald sich drei oder mehr Menschen mit dem Vorsatz verbinden, fortgesetzt gerichtlich strafbare Handlungen zu begehen (kriminelle Verbindung).

(2) Ein gefährlicher Angriff ist die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich um einen Straftatbestand
1. nach dem Strafgesetzbuch (StGB), BGBl. Nr. 60/1974, ausgenommen die Tatbestände nach den §§ 278, 278a und 278b StGB, oder
2. nach dem Verbotsgesetz, StGBl. Nr. 13/1945, oder
3. nach dem Fremdenpolizeigesetz 2005 (FPG), BGBl. I Nr. 100, oder
4. nach dem Suchtmittelgesetz (SMG), BGBl. I Nr. 112/1997,
handelt, es sei denn um den Erwerb oder Besitz eines Suchtmittels zum eigenen Gebrauch.

(3) Ein gefährlicher Angriff ist auch ein Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung (Abs. 2) vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird.

(4) Gefahrenerforschung ist die Feststellung einer Gefahrenquelle und des für die Abwehr einer Gefahr sonst maßgeblichen Sachverhaltes."

"2. TEIL
Aufgaben der Sicherheitsbehörden auf dem Gebiet der Sicherheitspolizei
1. Hauptstück

[...]

Gefahrenabwehr

§ 21. (1) [...]

(2) Die Sicherheitsbehörden haben gefährlichen Angriffen unverzüglich ein Ende zu setzen. Hiefür ist dieses Bundesgesetz auch dann maßgeblich, wenn bereits ein bestimmter Mensch der strafbaren Handlung verdächtig ist.

(3) [...]"

"4. TEIL
Verwenden personenbezogener Daten im Rahmen der Sicherheitspolizei
[...]
2. Hauptstück
Ermittlungsdienst"

"Zulässigkeit der Verarbeitung

§ 53. (1) Die Sicherheitsbehörden dürfen personenbezogene Daten ermitteln und weiterverarbeiten
1. für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§ 19);
2. für die Abwehr krimineller Verbindungen (§§ 16 Abs. 1 Z 2 und 21);
2a. für die erweiterte Gefahrenerforschung (§ 21 Abs. 3) unter den Voraussetzungen des § 91c Abs. 3;
3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenerforschung (§ 16 Abs. 4 und § 28a);
4. für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§ 22 Abs. 2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;
5. für Zwecke der Fahndung (§ 24);
6. um bei einem bestimmten Ereignis die öffentliche Ordnung aufrechterhalten zu können.

(2) Die Sicherheitsbehörden dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen verarbeitet haben, für die Zwecke und unter den Voraussetzungen nach Abs. 1 ermitteln und weiterverarbeiten; ein automationsunterstützter Datenabgleich im Sinne des § 141 StPO ist ihnen jedoch untersagt. Bestehende Übermittlungsverbote bleiben unberührt.

(3) […]

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskunft zu verlangen über
1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,
2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie
3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,

wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zu ihrer Lokalisierung zum Einsatz zu bringen. Die Sicherheitsbehörde trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens, dessen Dokumentation dem Betreiber unverzüglich, spätestens innerhalb von 24 Stunden nachzureichen ist. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und gegen Ersatz der Kosten nach § 7 Z 4 der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004, zu erteilen.

(3c) – (5) [...]"

"Pflicht zur Richtigstellung oder Löschung

§ 63. (1) Wird festgestellt, daß unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes ermittelte Daten aufbewahrt werden, so ist unverzüglich eine Richtigstellung oder Löschung vorzunehmen. Desgleichen sind personenbezogene Daten zu löschen, sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden.

(2) […]"

"6. TEIL
Rechtsschutz

[...]

3. Abschnitt

[...]

Befassung des Rechtsschutzbeauftragten

§ 91c. (1) Die Sicherheitsbehörden sind verpflichtet, den Rechtsschutzbeauftragten von jeder Ermittlung personenbezogener Daten durch Observation (§ 54 Abs. 2), durch verdeckte Ermittlung (§ 54 Abs. 3), durch den verdeckten Einsatz von Bild- oder Tonaufzeichnungsgeräten (§ 54 Abs. 4), durch Verarbeiten von Daten, die andere mittels Einsatz von Bild- und Tonaufzeichnungsgeräten er- und übermittelt haben (§ 53 Abs. 5) unter Angabe der für die Ermittlung wesentli-

chen Gründe in Kenntnis zu setzen. Für derartige Maßnahmen im Rahmen der erweiterten Gefahrenerforschung gilt Abs. 3. Darüber hinaus ist der Rechtsschutzbeauftragte über Auskunftsverlangen (§ 53 Abs. 3a Z 2 und 3, Abs. 3a zweiter Satz und 3b) sowie über den Einsatz von Kennzeichenerkennungsgeräten (§ 54 Abs. 4b) zu informieren.

(2) – (3) [...]

Rechte und Pflichten des Rechtsschutzbeauftragten

§ 91d. (1) Die Sicherheitsbehörden haben dem Rechtsschutzbeauftragten bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren, ihm auf Verlangen Abschriften (Ablichtungen) einzelner Aktenstücke unentgeltlich auszufolgen und alle erforderlichen Auskünfte zu erteilen; insofern kann ihm gegenüber Amtsverschwiegenheit nicht geltend gemacht werden. Dies gilt jedoch nicht für Auskünfte und Unterlagen über die Identität von Personen oder über Quellen, deren Bekannt werden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde, und für Abschriften (Ablichtungen), wenn das Bekannt werden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde.

(2) Dem Rechtsschutzbeauftragten ist jederzeit Gelegenheit zu geben, die Durchführung der in § 91c genannten Maßnahmen zu überwachen und alle Räume zu betreten, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden. Darüber hinaus hat er im Rahmen seiner Aufgabenstellungen die Einhaltung der Pflicht zur Richtigstellung oder Löschung nach § 63 oder den besonderen Löschungsbestimmungen zu überwachen.

(3) Nimmt der Rechtsschutzbeauftragte wahr, dass durch Verwenden personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Datenverwendung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus den Gründen des § 26 Abs. 2 des DSG 2000 nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzkommission nach § 90 befugt.

(4) […]"

3. Im gegebenen Zusammenhang interessierende Bestimmungen des Telekommunikationsgesetzes 2003 – TKG 2003, BGBl. I 70, lauten in der maßgeblichen (mit 19. Mai 2011 in Kraft getretenen) Fassung BGBl. I 27/2011: 11

"12. Abschnitt
Kommunikationsgeheimnis, Datenschutz
Allgemeines

§ 92. (1) Soweit dieses Bundesgesetz nicht anderes bestimmt, sind auf die in diesem Bundesgesetz geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, anzuwenden.

(2) Die Bestimmungen der Strafprozessordnung bleiben durch die Bestimmungen dieses Abschnittes unberührt.

(3) In diesem Abschnitt bezeichnet unbeschadet des § 3 der Begriff
1. 'Anbieter' Betreiber von öffentlichen Kommunikationsdiensten;
2. 'Benutzer' eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;
2a. 'Teilnehmerkennung' jene Kennung, welche die eindeutige Zuordnung eines Kommunikationsvorgangs zu einem Teilnehmer ermöglicht;
2b. 'E-Mail-Adresse' die eindeutige Kennung, die einem elektronischen Postfach von einem Internet-E-Mail-Anbieter zugewiesen wird;
3. 'Stammdaten' alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:
    a) Name (Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),
    b) akademischer Grad bei natürlichen Personen,
    c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen),
    d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
    e) Information über Art und Inhalt des Vertragsverhältnisses,
    f) Bonität;
4. 'Verkehrsdaten' Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;
4a. 'Zugangsdaten' jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind;
5. 'Inhaltsdaten' die Inhalte übertragener Nachrichten (Z 7);
6. 'Standortdaten' Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben;
6a. 'Standortkennung' die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-ID);
6b. 'Vorratsdaten' Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden;
7. 'Nachricht' jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

8. […];
9. 'Dienst mit Zusatznutzen' jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;
10.-13. […];
14. 'Internet-Zugangsdienst' einen Kommunikationsdienst im Sinne von § 3 Z 9, der in der Bereitstellung von Einrichtungen oder Diensten zur Erbringung von Zugangsleistungen zum Internet besteht;
15. [...];
16. 'öffentliche IP-Adresse' eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann. Öffentliche IP-Adressen sind Zugangsdaten im Sinne des § 92 Abs. 3 Z 4a. Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs. 3 Z 3.

Kommunikationsgeheimnis

§ 93. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung, der Überwachung von Nachrichten und der Auskunft über Daten einer Nachrichtenübermittlung einschließlich Vorratsdaten sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

(4) – (5) […]"

"Verkehrsdaten

§ 99. (1) Verkehrsdaten dürfen außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Die

Zulässigkeit der weiteren Verwendung von Verkehrsdaten, die nach Abs. 5 übermittelt werden, richtet sich nach den Vorschriften der StPO sowie des SPG.

(2) Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(3) – (4) […]

(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist zulässig zur Auskunft über
1. Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO;
2. Zugangsdaten, auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1, Abs. 3 Z 6 lit. a und b oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens sechs Monate vor der Anfrage gespeichert wurden, an Gerichte und Staatsanwaltschaften nach Maßgabe des § 76a Abs. 2 StPO.
3. Verkehrsdaten und Stammdaten, wenn hiefür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a und 3b SPG. Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung verarbeitet werden, auch wenn hiefür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist;
4. Zugangsdaten, auch wenn diese als Vorratsdaten gemäß § 102a Abs. 2 Z 1 oder § 102a Abs. 4 Z 1, 2, 3 und 5 längstens drei Monate vor der Anfrage gespeichert wurden, an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 3 SPG."

4. §§ 3 und 18 E-Commerce-Gesetz – ECG, BGBl. I 152/2001, haben folgenden Wortlaut: 12

"Begriffsbestimmungen

§ 3. Im Sinne dieses Bundesgesetzes bedeuten:
1. Dienst der Informationsgesellschaft: ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (§ 1 Abs. 1 Z 2 Notifikationsgesetz 1999), insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die

den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern;
2. Diensteanbieter: eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die einen Dienst der Informationsgesellschaft bereitstellt;
3. niedergelassener Diensteanbieter: ein Diensteanbieter, der eine Wirtschaftstätigkeit mittels einer festen Einrichtung auf unbestimmte Zeit tatsächlich ausübt, wobei das Vorhandensein und die Nutzung von technischen Mitteln und Technologien, die zur Bereitstellung des Dienstes erforderlich sind, für sich allein noch keine Niederlassung des Diensteanbieters begründen;
4. Nutzer: eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die zu beruflichen oder sonstigen Zwecken einen Dienst der Informationsgesellschaft in Anspruch nimmt, insbesondere um Informationen zu erlangen oder Informationen zugänglich zu machen;
5. Verbraucher: eine natürliche Person, die zu Zwecken handelt, die nicht zu ihren gewerblichen, geschäftlichen oder beruflichen Tätigkeiten gehören;
6. – 8. [...]"

"Umfang der Pflichten der Diensteanbieter

§ 18. (1) Die in den §§ 13 bis 17 genannten Diensteanbieter sind nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.

(2) Die in den §§ 13 und 16 genannten Diensteanbieter haben auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem alle Informationen zu übermitteln, an Hand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können.

(3) Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet.

(4) [...]

(5) Sonstige Auskunfts- und Mitwirkungspflichten der Diensteanbieter gegenüber Behörden oder Gerichten bleiben unberührt."

III. Erwägungen

Der Verfassungsgerichtshof hat über die – zulässige – Beschwerde erwogen: 13

1. Wie dargelegt, bekämpft der Beschwerdeführer Spruchpunkt 1. des angefochtenen Bescheides mit der Begründung, dass ihn vor allem die Ermittlung seiner IP-Adresse (aber auch Namen und Anschrift) ohne Einholung einer gerichtlichen Bewilligung in den verfassungsgesetzlich gewährleisteten Rechten auf Schutz des Fernmeldegeheimnisses gemäß Art. 10a StGG, allenfalls auch auf Geheimhaltung personenbezogener Daten nach § 1 DSG 2000 iVm Art. 8 EMRK verletze, die belangte Behörde zudem eine verfassungs- bzw. gleichheitswidrige Auslegung des Gesetzes vorgenommen, somit Willkür geübt und ihn daher im Recht auf Gleichheit aller Staatsbürger vor dem Gesetz (Art. 2 StGG, Art. 7 B-VG und Art. 14 EMRK) verletzt habe. 14

Obwohl die Erhebung der IP-Adresse des vom Beschwerdeführers benützten Endgerätes bei einer ex-ante-Betrachtung geradezu "geboten" gewesen sei, hätte der Vorgang einer gerichtlichen Bewilligung bedurft. Bei Daten darüber, "wann und mit welcher IP-Adresse mit welchem Nicknamen auf einem Chatserver kommunizierte wurde", handle es sich um Verkehrsdaten iSd § 93 Abs. 3 Z 4 TKG 2003, für deren Ermittlung der Betreiber seine Logfiles durchsuchen müsse. Derartige Auskünfte würden einen Eingriff in das gemäß Art. 10a StGG verfassungsgesetzlich geschützte Fernmeldegeheimnis bedeuten. Im Übrigen würden auch Stammdaten diesem Schutzbereich unterfallen. § 1 DSG 2000 und Art. 8 EMRK würden (obwohl nicht ausdrücklich statuiert) ebenfalls "zumindest eine gerichtliche Bewilligung von Eingriffen in das Fernmeldegeheimnis" erfordern. Bei verfassungskonformer Interpretation der Vorschrift des § 53 Abs. 3a Z 2 SPG wäre eine gerichtliche Anordnung einzuholen oder die Bestimmung "zugunsten des § 18 Abs. 2 ECG", der ebenfalls eine richterliche Anordnung verlange, "unangewendet zu lassen" gewesen. Sollte der Verfassungsgerichtshof die aufgezeigte grundrechtskonforme Interpretation nicht "für möglich erachten", wird die Einleitung eines Gesetzesprüfungsverfahrens bezüglich des § 53 Abs. 3a Z 2 SPG angeregt. 15

2. Gegen die Vorschriften des § 53 Abs. 3a Z 2 und 3 SPG sind vor dem Hintergrund des Falles keine verfassungsrechtlichen Bedenken entstanden. 16

3. Die in Rede stehenden Bestimmungen greifen aus folgenden Gründen nicht in den Schutz des Fernmeldegeheimnisses iSd Art. 10a StGG ein: 17

3.1. Die Verfassungsnorm des Art. 10a StGG wurde durch BGBl. 8/1974 in das StGG eingefügt; ihr zufolge darf das Fernmeldegeheimnis nicht verletzt werden (Abs. 1), Ausnahmen sind nur auf Grund eines richterlichen Befehls in Gemäßheit der bestehenden Gesetze zulässig (Abs. 2). 18

3.1.1. Beim Fernmeldegeheimnis handelt es sich nach den Gesetzesmaterialien um ein dem Briefgeheimnis "verwandtes Recht", das (wie Art. 10 StGG) die Vertraulichkeit aller "nicht für die Öffentlichkeit bestimmten, im Wege des Fernmeldeverkehrs übermittelten Nachrichten oder Mitteilungen" schützt (AB 960 BlgNR 13. GP, 2). Dabei kommt es auf die Bestimmung der Information für "eine konkrete Person" an, und nicht darauf, ob die Nachricht allgemein bekannt (geworden) ist. "Maßnahmen der rein technischen Überwachung des Fernmeldeverkehrs" stellen nach den zitierten Materialien keine Eingriffe in das Fernmeldegeheimnis dar, weil "ein geordneter und sicher funktionierender Fernmeldeverkehr ohne entsprechende betriebliche und technische Aufsicht nicht denkbar" sei. Dem Schutz unterliegt daher – wie beim Briefgeheimnis, das die Vertraulichkeit des Briefinhaltes (nicht allfällige Informationen auf dem Kuvert) garantiert – der weitergegebene Gedankeninhalt, ohne äußere Gesprächsdaten (zB Telefonnummern) zu erfassen. 19

3.1.2. Art. 10a StGG war bei seiner Einfügung in das Staatsgrundgesetz im Jahr 1974 primär auf den Telegraphen- und Fernmeldeverkehr ausgerichtet. Der Schutz ist nach herrschender Auffassung inzwischen nicht auf Telefonate und Telegramme beschränkt, sondern bezieht sich nunmehr – nicht zuletzt vor dem Hintergrund des dem Begriff "Fernmeldegeheimnis" bereits vom historischen Verfassungsgesetzgeber unterlegten weiten Verständnisses (AB 960 BlgNR 13. GP, 2) – auf alle Arten der Telekommunikation, einschließlich des Nachrichtenaustausches über das Internet (inklusive geschlossener Internetforen – Chat-Foren; vgl. mwN *Wiederin*, in: Korinek/Holoubek [Hrsg.], Österreichisches Bundesverfassungsrecht, 2001, Art. 10a StGG Rz 3 ff.; *Walter/Mayer/Kucsko-Stadlmayer*, Grundriss des österreichischen Bundesverfassungsrechts[10], 2007, Rz 1438; *Grabenwarter/Holoubek,* Verfassungsrecht – Allgemeines Verwaltungsrecht, 2009, Rz 473; *Grabenwarter*, Verfassung und Informationsgesellschaft, in: 20

Österreichische Juristenkommission [Hrsg.], Grundrechte der Informationsgesellschaft, 2001, 48 [65]).

Ob eine im Wege des Internets übermittelte Nachricht vom Schutzbereich des Art. 10a StGG erfasst ist, hängt also davon ab, ob es sich um eine Kommunikation handelt, die dem Telegraphen- und Fernmeldeverkehr entspricht. Der Nachrichtenaustausch ist daher jedenfalls dann geschützt, wenn bestimmte Teilnehmer miteinander kommunizieren wollen und die Nachricht jeweils nur für diese Teilnehmer bestimmt ist (es sich nach den Ausführungen der Bundesministerin für Inneres also um eine sogenannte geschlossene Kommunikation – wie etwa beim E-Mail-Verkehr – handelt).

3.1.3. Art. 10a StGG gewährleistet somit die Vertraulichkeit der Telekommunikation, schützt also jedenfalls den Inhalt einer auf diesem Weg weitergegebenen Nachricht, nicht aber sämtliche anderen damit zusammenhängenden Daten; Gegenstand des Fernmeldegeheimnisses sind somit alle Inhaltsdaten, nicht aber der gesamte Telekommunikationsverkehr schlechthin (vgl. auch *Wiederin*, aaO, Rz 11). 21

3.2. Seit Inkrafttreten der SPG-Novelle BGBl. I 114/2007 (mit 1. Jänner 2008) sind die Sicherheitsbehörden gemäß § 53 Abs. 3a SPG ermächtigt, auf Basis einer bestimmten Nachricht die dazugehörige (statische oder dynamische) IP-Adresse samt deren Verwendungszeit (Z 2) sowie anhand einer bestimmten IP-Adresse Namen und Anschrift des Nutzers des Endgerätes, dem die IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war (Z 3), zu ermitteln. 22

3.2.1. Die novellierten Bestimmungen fanden auf Grund eines Abänderungsantrages Eingang in das Gesetz (StenProtNR 23. GP, 42. Sitzung, 327 ff., insb. 330), dessen Begründung lautet: 23

"Durch diesen Abänderungsantrag soll den Bedenken des Datenschutzrates gegen Formulierungen und Regelungen der Regierungsvorlage Rechnung getragen werden.
Im Zusammenhang mit Z 4 (§ 53 Abs. 3a SPG) ist insbesondere auszuführen, dass die dort angeführten Daten den Sicherheitsbehörden zur Abwehr gefährlicher Angriffe oder zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht bereits jetzt zugänglich gemacht wurden. Nach den erhobenen Unterlagen handelt es sich dabei um Abfragen in der Größenordnung von etwa 1000 Anfragen pro Jahr. Es ist davon auszugehen, dass durch die nähere Umschreibung der den Sicher-

heitsbehörden im Sinne des § 53 Abs. 3a zur Verfügung zu stellenden Daten für die Betreiber öffentlicher Telekommunikationsdienste kein wesentlich gesteigerter Aufwand erwachsen wird."

3.2.2. Nach dem Wortlaut der Regelungen des § 53 Abs. 3a Z 2 und 3 SPG ist die Auskunftserteilung auf die einer bestimmten (der Sicherheitsbehörde zur Kenntnis gelangten) Nachricht zuzuordnende IP-Adresse bzw. auf Namen und Anschrift des Inhabers des zu einer bestimmten IP-Adresse gehörigen Endgerätes beschränkt, weshalb nur diese Daten seitens der Sicherheitsbehörde beim Betreiber oder sonstigen Diensteanbieter ermittelt werden dürfen. 24

Für die Erlangung anderer Daten bzw. Datenkategorien, insbesondere solcher, die über die schon bekannte Nachricht hinausgehende (durch Art. 10a StGG geschützte) Kommunikationsinhalte betreffen, enthält § 53 Abs. 3a SPG hingegen keine Ermächtigung. 25

3.2.3. § 53 Abs. 3a Z 2 SPG erlaubt den Sicherheitsbehörden die Ausforschung einer IP-Adresse ausschließlich auf Grund einer bestimmten, ihnen (wie hier) durch Mitteilung eines Kommunikationspartners oder durch offene (jedermann zugängliche) Internetkommunikation bekannt gewordenen Nachricht. 26

Die anhand einer solchen Nachricht unter den sonstigen Voraussetzungen des § 53 Abs. 3a Z 2 und 3 SPG seitens der Sicherheitsbehörde ermittelten (Einzel-)Daten sind daher nicht vom Schutzbereich des Art. 10a StGG erfasst. 27

3.2.4. Sobald also der Inhalt einer solchen Nachricht von den Sicherheitsbehörden aus einer offenen Kommunikation rechtmäßig ermittelt wurde oder aus einer geschlossenen Kommunikation von einem der Teilnehmer der Sicherheitsbehörde zugänglich gemacht wurde, steht sie daher nicht unter dem Schutz des Art. 10a StGG, sodass die Übermittlung der Verkehrsdaten, die in weiterer Folge die Ermittlung jener Personen, die an dem Nachrichtenverkehr teilgenommen haben, ermöglicht, nicht als Eingriff in das Fernmeldegeheimnis zu qualifizieren ist.

3.2.5. Die Vorschriften des § 53 Abs. 3a Z 2 und 3 SPG gestatten Sicherheitsbehörden somit von vornherein weder die geheime Überwachung des Internetverkehrs oder den Zugang zu einer Nachricht aus einem geschlossenen 28

Internetforum noch ermächtigen sie zur vorsorglichen anlasslosen Speicherung oder zur systematischen (etwa die Erstellung von Persönlichkeitsprofilen ermöglichende) Verknüpfung von Datensträngen, unabhängig davon, ob diese Daten auch dem Schutzbereich des Art. 10a StGG unterliegen (vgl. *Berka*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, Gutachten zum 18. Österreichischen Juristentag Bd I/1, 2012, 76 und 127).

3.2.6. Der Sicherheitsbehörde dürfen vom Betreiber vielmehr bloß punktuelle Auskünfte erteilt werden, die keinen Rückschluss auf andere (nicht bereits bekannte) Inhalte erlauben. 29

3.2.7. Die Auskunftsverpflichtung des Betreibers setzt überdies voraus, dass dieser überhaupt (noch) über gespeicherte Daten verfügt; eine über die Speicherverpflichtungen nach dem TKG (insbesondere zu Verrechnungszwecken gemäß § 99 Abs. 2 TKG 2003) hinausgehende Pflicht zur Speicherung von Verkehrsdaten enthält § 53 Abs. 3a SPG nicht (vgl. VfSlg. 18.830/2009). 30

3.3. Entgegen der Ansicht des Beschwerdeführers bieten die von der belangten Behörde im gegebenen Zusammenhang angewendeten Bestimmungen des § 53 Abs. 3a Z 2 und 3 SPG idF BGBl. I 114/2007 mithin keine Basis für die Ermittlung von Inhaltsdaten iSd Art. 10a StGG (vgl. VfSlg. 18.831/2009 [S 1137]; zu § 53 Abs. 3b SPG VfSlg. 18.830/2009). 31

4. Hingegen greift die Bestimmung des § 53 Abs. 3a SPG in das verfassungsgesetzlich gewährleistete Recht auf Datenschutz gemäß § 1 Abs. 1 DSG 2000 iVm Art. 8 EMRK ein, verletzt dieses jedoch aus folgenden Gründen nicht: 32

4.1. Nach § 1 Abs. 1 DSG 2000 hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf die Achtung des Privat- und Familienlebens, hat. 33

4.2. Beschränkungen dieses Grundrechts sind nach dem Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 (abgesehen von lebenswichtigen Interessen des Betroffenen an der Verwendung personenbezogener Daten oder seiner Zustimmung hiezu) bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und die aus- 34

reichend präzise, also für jedermann vorhersehbar regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten für die Wahrnehmung konkreter Verwaltungsaufgaben erlaubt ist (vgl. VfSlg. 16.369/2001, 18.146/2007, 18.963/2009, 18.975/2009). Der jeweilige Gesetzgeber muss somit nach den Vorgaben des § 1 Abs. 2 DSG 2000 – wie der Beschwerdeführer grundsätzlich zu Recht darlegt – eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden (VfSlg. 18.643/2008).

4.3. Eine solche ausdrückliche gesetzliche Ermächtigung zur Ermittlung der IP-Adresse sowie von Namen und Anschrift des Benutzers des Endgerätes, dem eine bestimmte IP-Adresse zugeordnet ist, enthält § 53 Abs. 3a Z 2 und 3 SPG. Der Eingriff ist auf die bloße Auskunftserteilung über die erfragten Daten beschränkt. Angesichts des im öffentlichen Interesse gelegenen Aufgabengebietes der Sicherheitsbehörden betreffend die Abwehr gefährlicher Angriffe, insbesondere iZm der Verhinderung der Verwirklichung unmittelbar bevorstehender Vorsatztaten nach dem StGB, dem Verbotsgesetz, dem Fremdenpolizeigesetz und dem Suchtmittelgesetz (§§ 16 Abs. 2 und 3, 21 Abs. 2 SPG), ist es auch nicht unverhältnismäßig, den Sicherheitsbehörden bei Vorliegen einer bestimmten Nachricht, welche die Annahme einer konkreten Gefahrensituation rechtfertigt, die Ermittlung der in Rede stehenden Daten im Wege des Betreibers oder sonstigen Diensteanbieters gemäß § 53 Abs. 3a Z 2 und 3 SPG (unter den Kautelen des kommissarischen Rechtsschutzes durch den weisungsfreien Rechtsschutzbeauftragten [§§ 91c ff. SPG] sowie konkreter Löschungsverpflichtungen [§ 63 SPG] – vgl. VfSlg. 18.831/2009 [S 1137 f.]) zu ermöglichen. 35

4.4. Im Übrigen ist eine richterliche Genehmigung staatlicher Überwachungsmaßnahmen durch Art. 8 EMRK nicht geboten (vgl. zB EGMR 10.2.2009, Fall *Iordachi*, Appl. 25.198/02, Z 40). 36

5. Der Beschwerdeführer ist daher durch den angefochtenen Bescheid nicht in Rechten wegen Anwendung eines von ihm als verfassungswidrig angesehenen Gesetzes verletzt worden. 37

6. Auch sind der belangten Behörde entgegen dem Beschwerdevorbringen bei Erlassung des angefochtenen Bescheides keine verfassungsrechtlich relevanten Vollzugsfehler unterlaufen: 38

6.1. Angesichts der verfassungsrechtlichen Unbedenklichkeit der angewendeten Rechtsvorschriften und des Umstandes, dass kein Anhaltspunkt dafür besteht, dass die Behörde diesen Vorschriften fälschlicherweise einen gleichheitswidrigen Inhalt unterstellt hat, könnte der Beschwerdeführer im verfassungsgesetzlich gewährleisteten Recht auf Gleichheit aller Staatsbürger vor dem Gesetz nur verletzt worden sein, wenn die Behörde Willkür geübt hätte. 39

Ein willkürliches Verhalten der Behörde, das in die Verfassungssphäre eingreift, liegt unter anderem in einer gehäuften Verkennung der Rechtslage, aber auch im Unterlassen jeglicher Ermittlungstätigkeit in einem entscheidenden Punkt oder dem Unterlassen eines ordnungsgemäßen Ermittlungsverfahrens überhaupt, insbesondere in Verbindung mit einem Ignorieren des Parteivorbringens und einem leichtfertigen Abgehen vom Inhalt der Akten oder dem Außer-Acht-Lassen des konkreten Sachverhaltes (zB VfSlg. 8808/1980 mwN, 14.848/1997, 15.241/1998 mwN, 16.287/2001, 16.640/2002). 40

6.2. Ausgehend vom plausibel festgestellten (unbestrittenen) Sachverhalt, wonach der Beschwerdeführer im Rahmen seines von einem Dritten offenbarten Internetauftritts bei der Sicherheitsbehörde den Eindruck erweckte, Unmündige im zeitlichen Konnex zu Sexualkontakten zu vermitteln, ist die Annahme der belangten Behörde, dass die gesetzlichen Voraussetzungen des § 53 Abs. 3a SPG für die getroffenen Maßnahmen (iSd Vorliegens einer auf Grund bestimmter Tatsachen indizierten Gefahrensituation sowie der Notwendigkeit der Datenermittlung als Voraussetzung für die Erfüllung sicherheitsbehördlicher Aufgaben) gegeben waren, verfassungsrechtlich nicht zu beanstanden. 41

Der Beschwerdeführer ist daher durch den angefochtenen Bescheid nicht im verfassungsgesetzlich gewährleisteten Recht auf Gleichheit aller Staatsbürger vor dem Gesetz verletzt worden. 42

6.3. Es ergeben sich auch keinerlei Anhaltspunkte dafür, dass der Eingriff in das verfassungsgesetzlich gewährleistete Recht auf Datenschutz nicht dem aus § 1 Abs. 2 DSG 2000 abzuleitenden Verhältnismäßigkeitsgrundsatz entsprach. 43

6.4. Der belangten Behörde ist bei Erlassung des angefochtenen Bescheides auch sonst kein in die Verfassungssphäre reichender Fehler unterlaufen: Der vom Beschwerdeführer relevierte § 18 Abs. 2 ECG bezieht sich nicht auf die Auskunftserteilung gemäß § 53 Abs. 3a SPG (§ 18 Abs. 5 ECG) und wurde daher zu Recht nicht angewendet. 44

IV. Ergebnis und damit zusammenhängende Ausführungen

1. Die behauptete Verletzung verfassungsgesetzlich gewährleisteter Rechte hat sohin nicht stattgefunden. 45

2. Das Verfahren hat auch nicht ergeben, dass der Beschwerdeführer in von ihm nicht geltend gemachten verfassungsgesetzlich gewährleisteten Rechten verletzt wurde. Angesichts der Unbedenklichkeit der angewendeten Rechtsgrundlagen ist es auch ausgeschlossen, dass er in seinen Rechten wegen Anwendung einer rechtswidrigen generellen Norm verletzt wurde. 46

3. Die Beschwerde war daher abzuweisen. 47

4. Diese Entscheidung konnte gemäß § 19 Abs. 4 erster Satz VfGG ohne mündliche Verhandlung in nichtöffentlicher Sitzung getroffen werden. 48

Wien, am 29. Juni 2012
Der Präsident:
Dr. HOLZINGER

Schriftführerin:
Dr. WEINHANDL